La Revue des droits de l'homme
Revue du Centre de recherches et d'études sur les droits fondamentaux
Actualités Droits-Libertés | 2015

Sans doigt, ni loi : La CJUE donne son « feu vert » à la biosurveillance

Protection des données personnelles (CJUE)

Jean-Philippe Foegle

Édition électronique
URL : http://journals.openedition.org/revdh/1394
DOI : 10.4000/revdh.1394
ISSN : 2264-119X

Éditeur
Centre de recherches et d'études sur les droits fondamentaux

Référence électronique
Jean-Philippe Foegle, « Sans doigt, ni loi : La CJUE donne son « feu vert » à la biosurveillance », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 28 juillet 2015, consulté le 30 avril 2019. URL : http://journals.openedition.org/revdh/1394 ; DOI : 10.4000/revdh.1394

Sans doigt, ni loi : La CJUE donne son « feu vert » à la biosurveillance

Protection des données personnelles (CJUE)

Jean-Philippe Foegle

1 « Pas de bras, pas de chocolat » : l'expression teintée d'humour noir désormais passée dans le langage courant fait toujours recette, comme en témoigne un récent film à succès. Et, si l'humour n'est pas systématiquement chose la mieux partagée, l'efficace simplicité de cet adage semble exercer un pouvoir de séduction tel que son écho résonne jusque dans les enceintes de l'Union Européenne. *« Pas de doigt, pas de droit »* : ainsi pourrait être résumé, par analogie comique, l'apport brut de l'arrêt Willems au régime européen de protection des données personnelles – et, accessoirement, au registre de l'humour juridictionnel.

2 L'affaire en cause concernait l'usage des données biométriques des passeports collectées sur le fondement du règlement (CE) n° 2252/2004 du Conseil, du 13 décembre 2004[1]. Elle avait pour point de départ une demande de décision préjudicielle portant sur l'interprétation des articles 1er, paragraphe 3[2], et 4, paragraphe 3[3], du règlement en cause, présentée dans le cadre des litiges opposant le requérant aux autorités publiques néerlandaises. Le litige s'était élevé au sujet du refus de ces dernières de délivrer respectivement aux requérants un passeport (affaires C-446/12, C-448/12 et C-449/12) et une carte d'identité (affaire C-447/12) faute pour ceux-ci d'avoir **consenti au recueil de leurs empreintes digitales**. Selon les requérants, la saisie et la conservation de leurs empreintes constituerait une atteinte importante à leur intégrité physique et à leur droit à la protection de la vie privée, atteinte qui résulterait notamment - et c'est bien là que réside le « nœud gordien » du litige - de ce que les autorités pourraient utiliser lesdites empreintes **à des fins ultérieures de celles pour lesquelles ils les ont fournies, en particulier à des fins judiciaires.**

3 La question préjudicielle renvoyée par la juridiction néerlandaise comportait trois questions distinctes. La première, qui portait sur la compatibilité du règlement aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne avait déjà été

résolue précédemment en 2013 par un arrêt Schwartz[4] et a donc été retirée. Les deux secondes ont en revanche été maintenues. La première question portait sur l'applicabilité du règlement aux demandes de cartes d'identité. La seconde et plus importante portait, quant à elle, sur l'interprétation proprement dite du règlement : Celui-ci oblige-t-il les États membres à **garantir que les données biométriques rassemblées ne seront pas utilisées à d'autres fins autres que la délivrance du passeport ou du document de voyage** ? Et, dans le cas contraire, une telle utilisation ultérieure serait-elle compatible avec la directive 95/46/CE ainsi qu' avec les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne garantissant respectivement aux justiciables le droit a la vie privée et un droit autonome a la protection des données personnelles ?

4 Posant en creux l'épineuse question de la limitation de **l'usage par les pouvoirs publics des données biométriques à des fins de surveillance**, la décision de la Cour de justice dans l'affaire Willems suscitait de nombreuses attentes[5]. L'enjeu était en effet de taille : il s'agissait, ni plus ni moins, que de préserver le **sens et la portée de la protection européenne des données personnelles en matière de biométrie**. En effet, par leur caractère hautement sensible, ces données se trouvent placées au cœur du droit à la protection de la vie privée-intimité en son sens le plus ancien[6], de sorte que tout reflux de la protection des données personnelles en la matière ne peut que passer pour une atteinte particulièrement grave au fragile socle de protection de la vie privée. Définies par le G29 comme des données portant sur « des propriétés biologiques, des aspects comportementaux, des caractéristiques physiologiques, des caractéristiques vivantes ou des actions reproductibles lorsque ces caractéristiques et/ou actions sont à la fois propres à cette personne physique et mesurables »[7] celles-ci ont pour particularité de rendre des caractéristiques physiques permanentes d'une personne « lisibles par une machine »[8] et de permettre le profilage des individus en les plaçant dans des catégories prédéterminées, très souvent à leur insu. Plus concrètement, les risques liés à l'explosion de l'usage de ces donnée sont nombreux et ont été soulignées tant par le contrôleur européen des données[9] que par le G29[10] et la CNIL[11]. Le droit a certes d'ores et déjà tenté d'encadrer le phénomène : au niveau de la « Grande Europe », le retentissant arrêt Marper c. Royaume-Uni[12] a énonce que le simple fait de conserver ou collecter ce type de données doit « passer pour emporter des conséquences directes sur la vie privée de l'individu concerné, que ces données soient utilisées par la suite ou non ».

5 Les risques de profilage des individus suscités par la collecte de données biométriques sont d'autant plus préoccupants que ceux-ci, portent le risque de « stigmatisation »[13] des personnes visées lorsque ces données sont utilisées à des fins de police et stockées sur dans des bases centralisées. C'est **précisément cette éventuelle constitution de grandes bases de données aux fins de police qui préoccupait à juste titre les requérants et fondait l'enjeu pratique du litige**. Et c'est, soulignons-le, ces risques qui avaient occupé les débats autour de l'adoption du règlement. L'objectif de cette proposition de la commission introduite le 18 février 2004 était de rendre les passeports plus « sûrs » en instaurant un instrument juridiquement obligatoire relatif aux normes concernant les dispositifs de sécurité harmonisés, notamment en vue de se conformer au programme Nord-Américain d'exemption de visa - mais également, plus subtilement, de contribuer à la mise en œuvre des « frontières intelligentes » dont la commission se veut fervente défenseresse.

6 La proposition de règlement de la Commission[14] offrait initialement la possibilité explicite de stocker les empreintes digitales dans une base de données nationale en vue de la

création d'un futur registre européen des documents délivrés. Cette proposition **avait suscité l'ire du parlement européen** qui, par une résolution législative[15] à caractère non contraignant avait **émis de nombreuses réserves sur cette proposition.** Un amendement du même parlement avait introduit un amendement précisant qu'« il n'est établi aucune base de données centralisée des passeports et documents de voyage de l'Union européenne contenant les données biométriques et autres de tous les titulaires d'un passeport au sein de l'UE », tandis que le rapport de la Commission des libertés civiles, de la justice et des affaires intérieures du 25 octobre 2004, avait estimé que « la création d'une base de données centralisée violerait les principes de finalité et de proportionnalité », et conduirait à accroître le risque d'abus et de dérapages en augmentant le « risque d'utilisation des éléments d'identification biométrique comme « clés d'accès » à diverses bases de données, mettant ainsi en connexion différents fichiers »[16]. Le Conseil n'avait néanmoins pas tenu compte des suggestions et demandes de modification du Parlement, et le règlement entré en vigueur le 18 janvier 2005 n'incluait pas explicitement l'interdiction de la constitution de bases de données centralisées contenant les données biométriques. Il revenait donc aux juges de Luxembourg, et à eux-seuls, de **confirmer ou d'infirmer les craintes exprimées par le Parlement Européen**. Et, en somme, d'ouvrir la voie à une **réutilisation massive des données collectées dans le cadre de la gestion des frontières européennes**, ou, au contraire, de garantir pleinement aux citoyens la protection de leurs données personnelles.

7 Répondant à la question renvoyée par la juridiction de renvoi, la CJUE énonce que l'article 4, paragraphe 3, du règlement n° 2252/2004, n'oblige pas les États membres à garantir que les données biométriques rassemblées et conservées sur le fondement dudit règlement ne seront pas rassemblées, **traitées et utilisées à des fins autres que la délivrance du passeport ou du document de voyage**. Surtout - et par un raisonnement pour le moins spécieux - la Cour ne place les données biométriques en cause **ni sous l'empire de la Charte des droits fondamentaux de l'Union Européenne, ni sous celui de la directive 1995/46/CE protégeant les données personnelles.**

8 Ce faisant, la Cour se défausse très largement de ses responsabilités en la matière, a **ffaiblissant considérablement la force et l'unité du régime européen de protection des données personnelle** et renvoyant de ce fait la balle à la Cour européenne des droits de l'homme et aux États-membres s'agissant de la définition d'un niveau de protection acceptable contre la « biosurveillance ». **(1°)**.

9 Plus largement, en refusant pour des motifs largement légalistes - peu convaincants à notre sens - de faire application de la Charte des droits fondamentaux et de la directive 95/46/CE, la Cour introduit des incertitudes **supplémentaires quant à la portée de la protection des droits de l'homme et particulièrement du droit à la vie privée dans l'ordre juridique de l'Union européenne**. Il apparaît par conséquent bien difficile voire impossible de déterminer avec précision la substance de la protection de la vie privée accordée aux justiciables européens tant la démarche de la Cour apparaît traversée de contradictions et d'incohérences. Signe sans doute que la marche vers la « constitutionnalisation » supposée du droit à la vie privée dans l'ordre juridique de l'Union n'est pas, loin s'en faut, une marche triomphale. **(2°)**

1°/- Un « feu vert » européen à la constitution de bases de données biométriques par les Etats-Membres

10 En refusant de manière contestable de confronter au régime européen de protection des données personnelles les usages des données biométriques collectées dans le cadre du règlement 2252/2004, la CJUE affaiblit considérablement l'efficacité et la cohérence du régime européen de protection des données personnelles (A). En conséquence, l'appréciation de la compatibilité de l'usage et du recueil de ces données sensibles reste donc, désormais, à la charge de la Cour européenne des droits de l'Homme et des Etats membres[17] (B).

A – Un affaiblissement contestable du régime européen de protection des données personnelles en matière de biométrie

11 Le règlement 2252/2004[18] n'a, à l'exception notable de l'arrêt « Schwarz » de 2013[19], qu'assez peu mobilisé les juges de Luxembourg. La question posée par la juridiction de renvoi dans le précédent arrêt Schwarz différait cependant en partie de l'affaire en cause, car elle concernait la conformité du règlement à la Charte des droits fondamentaux *stricto-sensu*. Après avoir écarté les arguments relatifs à l'absence de base juridique du règlement et du vice tiré de la prétendue absence de consultation du Parlement Européen, la Cour y avait affirmé la conformité du règlement aux articles 7 et 8 de la Charte de droits fondamentaux de l'Union Européenne. Ce faisant, la CJUE n'avait, soulignons-le, **accordé aucun blanc seing aux autorités nationales** en matière de collecte des données biométriques : bien au contraire, la conformité du règlement à la Charte des droits fondamentaux de l'UE avait été subordonnée à de nombreuses garanties.

12 En premier lieu, la Cour avait conclu à l'existence d'une atteinte au droit à la vie privée en rappelant, à la suite des arrêts *« Asnef »*[20] et *« Volker und Markus Schecke »*,[21] que le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel *« se rapporte à toute information concernant une personne physique identifiée ou identifiable »* Puis, citant l'arrêt *Marper*[22] de la CEDH, les juges de Luxembourg avaient précisé que **les empreintes digitales se rattachent indéniablement à la notion de *« vie privée »*** dès lors qu'elles contiennent objectivement « *des informations uniques sur des personnes physiques et permettent leur identification précise* »

13 Par la suite, rappelant que les articles 7 et 8 de la Charte ne constituent pas des prérogatives absolues et *« doivent être pris en considération par rapport à leur fonction dans la société »*[23], la Cour avait conclu au **caractère justifié et proportionné de l'atteinte en émettant de nombreuses réserves**, et ce en trois étapes. Après avoir constaté de manière curieusement rapide[24] que l'ingérence était bien « prévue par la loi », les juges en étaient venus aisément à la conclusion que le règlement poursuivait bien *« un objectif d'intérêt général reconnu par l'Union »*, visant notamment à empêcher l'entrée illégale de personnes sur le territoire de l'Union en prévenant la falsification des passeports et leur utilisation frauduleuse[25]. Restait alors à examiner si les moyens mis en œuvre par le règlement n'allaient pas au delà de ce qui apparaît nécessaire pour atteindre les buts

poursuivis. Sur ce point, la Cour avait notamment énoncé que le prélèvement de l'empreinte de deux doigts n'entraîne pas de désagrément physique ou psychique particulier pour l'intéressé, à l'instar de la prise de sa photo faciale, et présentait un degré d'efficacité acceptable[26]. Mais surtout, dans un second temps, les juges avaient rappelé, en citant à nouveau l'arrêt Marper[27], que le législateur doit *« **s'assurer qu'il existe des garanties spécifiques** visant à protéger ces données efficacement contre les traitements impropres et abusifs »*. De manière plus pertinente encore au regard de l'arrêt Willems, la Cour avait souligné que le règlement ne pouvait **d'aucune manière servir de base juridique à une éventuelle centralisation des données collectées sur son fondement ou à l'utilisation de ces dernières à d'autres fins que celles prévues par le règlement**. Par conséquent, la compatibilité au règlement d'une législation prévoyant une base centralisée des empreintes digitales devrait être examinée à l'occasion d'un recours devant les juridictions nationales[28].

14 Les conclusions de l'avocat général permettent d'éclairer le raisonnement suivi par la Cour. Celui-ci, tout en admettant qu*« il [n'est pas possible] d'exclure, de manière absolue, tout risque, y compris en termes d'utilisation frauduleuse et de contrefaçon. »*, avait conclu que le risque en cause n'était pas suffisant pour emporter invalidation du règlement, et ce notamment parce que les empreintes digitales ne sont utilisées *« que pour vérifier »* l'authenticité du passeport[29]. L'avocat général avait d'ailleurs insisté sur le fait que si le règlement est bien conforme aux articles 7 et 8 de la Charte des droits fondamentaux de l'UE, ce n'est **qu'en raison du caractère modeste de l'atteinte à la vie privée qu'il permet de mettre en œuvre**, atteinte limitée à l'identification des titulaires des passeports par le biais de leurs empreintes digitales.[30]

15 A ce stade, il y avait deux *« clés de lecture »* de la conformité du règlement aux articles 7 et 8 de la Charte. Il était certes possible de voir d'ores et déjà dans l'arrêt Schwartz une tendance de la Cour à se défausser de ses responsabilités sur les Etats-membres, puisque l'avocat général avait dénié que le règlement soit *« la cause de l'exposition des citoyens de l'Union au risque d'abus encouru dans ces États »*[31] et que l'arrêt lui-même avait énoncé que les risques liés à l'éventualité d'une centralisation, des données n'était *« pas de nature à affecter la validité dudit règlement « .* Il serait alors envisageable de conclure que la Cour avait tout simplement constaté que le règlement n'avait **pas offert de base juridique à la centralisation ultérieure de ces données**, plaçant *de facto* ce type d'utilisation hors du champ d'application du droit de l'Union mais laissant toute latitude aux Etats membres pour agir de la sorte. Mais il était également possible, par un effort minime de reconstruction du raisonnement des juges et d'interprétation (légèrement) constructive du droit primaire, de constater que ceux-ci n'avaient conclu à la conformité du règlement qu'**après avoir longuement insisté sur la nécessité de respecter les principes énoncés par l'arrêt « *Marper c. Royaume-Uni* »** et en se fondant, notamment, sur le constat d'une finalité du règlement limitée au contrôle de l'authenticité des passeports ainsi que sur la circonstance qu' *« en principe, le citoyen de l'Union est le seul détenteur de l'image de ses empreintes «*[32] . Dès lors, il était possible d'envisager que toute utilisation ultérieure des données se trouverait grevée d'une forte présomption de non-conformité au droit primaire de l'Union Européenne.

16 C'est néanmoins à une interprétation minimaliste des principes de l'arrêt Schwartz que s'est livrée la Cour dans le jugement Willems. En effet, dans l'arrêt commenté, les juges ont purement et simplement énoncé que *« lesdites utilisation et conservation des données ne sont pas régies par ce dernier règlement »* car celui-ci « *ne saurait constituer une base juridique*

pour établir ou maintenir, dans les États membres, des bases de données stockant ces informations, puisque cet aspect relève de la compétence exclusive des États membres. »[33]. Par conséquent, est énoncé que le règlement n° 2252/2004 **n'oblige pas un État membre à garantir aux citoyens que les données biométriques ne seront *« ni utilisées ni conservées par cet État à des fins autres* »** que celle de l'identification des titulaires du passeport[34].

17 Il y a en outre un aspect particulièrement spécieux dans le raisonnement mené par les juges luxembourgeois dans l'arrêt Willems, vivement dénoncé par Steve Peers[35] : le fait que ceux-ci n'aient **aucunement fait application de l'article 6.1,b) de la directive 95/46/CE**[36], qui garantit la limitation des finalités aux traitements de données[37].

18 Ce refus d'appliquer la directive est justifié, au yeux de la Cour, par le fait que la Cour n'a demandé que l'interprétation du règlement 2252/2004 à l'exclusion de tout autre texte de droit dérivé. Or, une **lecture sommaire de l'arrêt permet de s'apercevoir que ce raisonnement est, purement et simplement erroné**. Il apparaît en effet par ses questions préjudicielles, la juridiction de renvoi a bel et bien demandé l'interprétation de l'*« article 4, paragraphe 3, du règlement [n° 2252/2004], [lu] à la lumière de l'article 7, partie introductive et sous f), de la directive [95/46] , lus en combinaison avec l'article 6, paragraphe 1, partie introductive et sous b), de cette directive »*[38]. Et, comme le souligne à juste titre Steve Peers, le fait que la juridiction ait ou non demandé l'interprétation de la directive importe peu, puisque la CJUE a **très souvent reformulé les questions posées par les États membres en vue d'apporter une réponse complète aux enjeux de droit européen** soulevés par les juridictions nationales. Ainsi, dans l'affaire *Promusicae*[39], qui concernait la collecte de masse des données des internautes dans le but de protéger les droits de propriété intellectuelle des éditeurs, la juridiction de renvoi n'avait *stricto sensu* demandé l'interprétation que de la directive « e-commerce »[40], et cela n'avait nullement constitué un obstacle à ce que la CJUE reformule la question pour examiner la compatibilité de la législation nationale en cause au regard d'une autre directive pertinente, la directive « e-privacy[41] ».

19 Or, celle-ci aurait pu, précisément, ouvrir la voie à une censure d'une telle utilisation des empreintes digitales recueillies sur le fondement du règlement. D'une part, dans l'arrêt Schwartz, la Cour avait d'ores et déjà énoncé que le recueil d'empreintes digitales doit être conçu comme *« constituant un traitement de données à caractère personnel »*[42] au sens de la directive 95/46/CE, plaçant ce type de traitement de données sous l'empire de la directive 95/46/CE. Et surtout, d'autre part, la CJUE comme le G29 avaient déjà érigé le principe de finalités déterminées du traitement de données personnelle au rang de principe fondamental du régime européen. Marquant la prise en compte de *« l'exigence de prévisibilité des traitements de données »*[43], le principe de détermination de finalités limitées implique nécessairement que ***« la collecte des données à caractère personnel et ses modalités, ainsi que les finalités, doivent être décidées au préalable »*** tout traitement ultérieur incompatible avec les finalités prédéfinies étant interdit[44]. Dans son avis 03/2013[45], le G29 avait précisément exprimé des inquiétudes quand au recul de principe de spécification des finalités du traitement et mis en place une grille de lecture permettant de sauvegarder les garanties liées à la détermination de ces finalités.

20 Soulignant que l'utilisation de données à des fins différentes de celles initialement prévues ne rend pas nécessairement cette utilisation illégale - sauf à interdire totalement tout usage à fin scientifique de ces données ou à faire du « big data » une coquille vide - le groupe avait néanmoins instauré une grille de lecture en 4 étapes permettant d'entourer de garanties ce type d'usages ultérieurs des données. Il s'agit en premier lieu, d'une part,

d'examiner la relation entre les finalités poursuivies par la collecte initiale et la les finalités poursuivies par l'usage ultérieur des données, qui **ne doivent pas *a priori* présenter un lien trop ténu et devraient contribuer aux mêmes buts**[46]. D'autre part, il s'agit également d'examiner le contexte dans lequel la collecte de données est effectuée, et notamment le fait que la personne dont les données ont été collectées **puisse ou non raisonnablement s'attendre à ce que ses données soient réutilisées par la suite.** Dans ce cadre, comme le souligne le G29, plus la collecte est ciblée est spécifique, plus le titulaire des données doit pouvoir raisonnablement s'attendre à ce que ses données ne soient pas réutilisées[47]. En second lieu, il s'agit d'une part d'être attentif aux risques - notamment les risques de dissémination des données - que suscite la réutilisation des données, ce qui implique d'autre part que soit portée une attention particulière à la mise en sécurité des données[48].

21 Cette grille de lecture de l'article 6 de la directive 95/46 aurait sans nul doute, *a minima*, conduire la Cour à grever d'une forte présomption de non-conformité au droit de l'Union européenne toute utilisation ultérieure des données collectées dans le cadre du règlement de 2004. En effet, le caractère extrêmement spécifique et ciblé de la collecte d'empreintes digitales pouvait **indubitablement générer dans l'esprit des requérants une « *attente raisonnable* »** que leurs données ne fassent pas l'objet d'un traitement plus étendu et plus attentatoire à la vie privée par la suite[49] .

22 En refusant d'examiner l'affaire au regard de la directive 95/46/CE, la CJUE a certes maintenu une cohérence factice de sa jurisprudence. Mais elle a surtout ouvert la « boîte de Pandore » et **affaibli de manière considérable le régime protecteur des données personnelles de nature biométrique.** Il s'agit là d'une abstention d'autant plus dommageable qu'elle conduit dès lors à faire reposer la protection des données biométriques des citoyens européens sur une jurisprudence strasbourgeoise incertaine et sur des pratiques nationales pour le moins hétérogènes.

B – La Cour européenne des droits de l'homme, dernier rempart contre la biosurveillance ?

23 S'agissant des garanties contre les usages abusifs ou dangereux des données biométriques, la Cour a conclu dès l'arrêt *Leander c. Suède*[50] que le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 de la CEDH, que ces informations soient ou non utilisées par la suite[51]. Dans ce cadre, la Cour tient compte du contexte de la mémorisation des données et de la nature de celles-ci, ainsi que de la manière dont elles sont utilisées et traitées[52]. A cet égard, les juges de Strasbourg accordent une importance particulière au **caractère identifiant des données collectées :** dans l'affaire *P.G. et J.H. c. Royaume-Uni*[53] , la Cour avait observé que l'enregistrement de la voix d'une personne sur un support permanent en vue d'une analyse ultérieure permettait manifestement l'identification de cette personne. Elle avait donc jugé en conséquence que l'enregistrement des voix des requérants en vue d'une telle analyse ultérieure avait porté atteinte à leur droit au respect de leur vie privée. La solution a été étendue par la suite aux empreintes digitales dans l'arrêt *Marper c. Royaume-Uni*, car celles-ci *« contiennent objectivement des informations uniques sur l'individu concerné et permettent une identification précise dans un grand nombre de circonstances. ».*[54]

24 Certes, la circonstance qu'une collecte de donnée constitue une ingérence dans le droit à la vie privée n'implique pas nécessairement que cette atteinte soit injustifiée. D'une part, l'ingérence doit être « prévue par la loi » au sens de l'article 8 de la convention, ce qui signifie que la collecte massive de données biométriques en vue de la constitution de bases de données de police doit s'accompagner, **d'un minimum d'exigences** concernant *« la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire »*[55]. Force est néanmoins de constater que la Cour a apprécié de manière souple ces exigences dans son arrêt *Marper c. Royaume-Uni* en notant que ces aspects sont *« étroitement liés à la question plus large de la nécessité de l'ingérence dans une société démocratique »*[56].

25 S'agissant ainsi de l'appréciation du caractère nécessaire d'une atteinte, la Cour insiste sur le fait que les garanties entourant le traitement de données personnelles aux fins de police sont particulièrement nécessaires *« lorsqu'est en jeu la protection de catégories particulières de données plus sensibles »*, ce qui implique une attention soutenue l'égard de l'usage par les pouvoirs publics de données collectées sans le consentement des personnes concernées, notamment des données ADN qui, dans la mesure où elles contiennent le patrimoine génétique de la personne, revêtent une grande importance tant pour elle-même que pour sa famille[57]. A cet égard, la collecte indifférenciée de données biométriques aux fins de police devrait particulièrement attirer l'attention des juges en ce qu'elle est porteuse d'**un *« risque de stigmatisation »***, des personnes n'ont été reconnus coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence.

26 La nécessité de définir des finalités déterminées aux traitements de données apparaît, quant à elle, moins claire dans la jurisprudence de la Cour européenne des droits de l'homme : en effet, l'exigence de fixation de finalités déterminées relève en tant que tel du **socle d'exigences techniques propres au droit à la protection des données personnelles** et non de la notion de vie privée en tant que telle[58]. La notion d' « *aspiration raisonnable à la vie privée* » à laquelle se réfère - implicitement ou explicitement - la jurisprudence de la Cour depuis 2005[59] tend néanmoins à instaurer à la charge des gestionnaires du traitement une obligation de **respecter les finalités initialement déterminées lors de la collecte des données personnelles** . Ce concept - dont l'on doit la paternité à l'arrêt Katz de la Cour Suprême des Etats-Unis en 1964[60] - comporte un double élément objectif et subjectif. Sur le plan subjectif, il s'agit d'examiner si l'individu dont la vie privée avait pu être convaincu du caractère privé d'un lieu ou de l'un de ses comportements. Sur le plan objectif, est généralement exigé que le comportement en cause soit conçu par la société toute entière comme privé et non public. La Cour a appliqué de manière explicite ce test d' *« aspiration raisonnable à la vie privée »* dans de nombreuses hypothèses depuis l'arrêt *Halford c. Royaume-Uni* de 1997[61], notamment dans le cadre de contentieux sur la vie privée au travail[62] et la collecte de données issues de comportements s'étant déroulés dans un lieu public. De manière extrêmement significative, la Cour a conclu dans l'arrêt *Peck c. Royaume-Uni* à l'existence d'une violation de la vie privée d'un requérant dont la tentative de suicide avait été filmée à son insu par un dispositif de vidéosurveillance puis divulguée dans divers médias au motif que sa tentative de suicide *« avait été diffusée à une échelle dépassant de loin ce que le requérant aurait pu légitimement prévoir »*[63].

27 Il n'est à ce stade pas déraisonnable d'affirmer que la notion d' *« aspiration raisonnable à la vie privée »* utilisée par la Cour implique nécessairement **que les finalités assignées à un traitement de données soit explicites et limitées,** et que les usages ultérieurs de ses données soient strictement contingentés. En effet, un citoyen dont les données seraient collectées en vue de la confection d'un passeport sécurisé pourrait sans nul doute se prévaloir d'une aspiration raisonnable à ce que ses données ne soient pas utilisées à d'autres fins, et notamment à des fins de constitution de bases de données de police. Au-delà, il paraît également faire peu de doute que la limitation des finalités assignées aux données participe, comme le rappelait l'avocat général Kokott, d'**une exigence plus large de transparence et de prévisibilité des traitement de données personnelles**[64]. Or, cette exigence de prévisibilité est commune au droit de l'Union européenne et au droit de la Convention européenne des sauvegarde des droits de l'homme, les juges ayant à de nombreuses reprises rappelé aux Etats membres la nécessité de rédiger les lois *« avec assez de précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite »*[65].

28 Au vu des éléments précédemment cités, il paraît plausible voire probable qu'une législation nationale autorisant la centralisation de données biométriques à des fins de surveillance policière aurait bien peu de chance de passer le « cap » du contrôle des juges de Strasbourg sur le fondement de l'article 8 de la convention. Soulignons néanmoins que la jurisprudence de la Cour reste très casuistique et timide, voire timorée sur la question de la surveillance de masse[66]. Surtout, les rares garde-fous mise en place par la Cour insistent essentiellement sur la « prévisibilité » des atteintes à la vie privée trouvant leur fondement dans la réutilisation de données à des finalités autres que celles pour lesquelles elles ont été collectées, ce qui ne **correspond pas parfaitement au principe de détermination des finalités tel qu'il existe en droit de l'Union européenne**.

29 Or, dans la mesure où la CJUE a précisément énoncé dans ses arrêts *Schwartz* et *Willems* que le règlement n'interdit aucunement en tant que tel la réutilisation des données collectées en vue de fabriquer des passeports, les Etats-membres ont à ce stade pleine latitude pour mettre en œuvre une législation remplissant les conditions minimales de prévisibilité énoncées par la jurisprudence. Dans ce cadre, une définition minimaliste des hypothèses dans lesquelles les données biométriques collectées pourraient être réutilisées à des fins de surveillance pourrait être suffisante, dans la mesure où, comme l'a rappelé la Cour dans son arrêt *Malone*[67], **l'exigence de prévisibilité de la législation n'est pas aussi élevée dans les hypothèses de surveillance policière** que dans les autres hypothèses d'atteinte à la vie privée puisque, par définition, une mesure de surveillance policière vise à observer les comportements de celle-ci à son insu.

*

30 Ayant refusé d'encadrer les usages des données biométriques collectées sur le fondement du règlement en litige par une lecture minimaliste de son arrêt *Schwartz,* la CJUE s'est de se fait **« *lavé les mains* »** des risques de biosurveillance suscités par l'usage de la biométrie dans le cadre de la gestion des frontières de l'UE[68].

31 Mais le jugement *Willems* suscite un malaise plus profond et révèle des enjeux plus larges. A l'heure où la CJUE est amenée à se prononcer sur l'eurocompatibilité du *« safe harbour »* [69], son interprétation très restrictive de la Charte des Droits fondamentaux en matière de

vie privée semble bien marquer le *glas* de la démarche constructive des juges de Luxembourg en matière de protection des données personnelles.

*

2°/- Un jugement marquant le « glas » de la démarche constructive de la CJUE en matière de protection des données personnelles ?

32 Refusant de bouger le petit doigt pour protéger de manière effective les données personnelles des justiciables dans un domaine où cette protection est particulièrement nécessaire, la CJUE crée une incertitude supplémentaire sur la portée de la Charte des Droits Fondamentaux **(A).** Au-delà, ce sont en particulier les articles 7 et 8 de la Charte des droits fondamentaux dont la portée apparaît susceptible d'être réduite. Le présent jugement paraît donc bien sonner le glas de la jurisprudence constructive de la CJUE en matière de protection de la vie privée **(B)**.

A – Un reflux supplémentaire de la portée de la Charte des droits fondamentaux

33 Le raisonnement mené dans l'arrêt conduit, une fois n'est pas coutume, à renforcer l'incertitude sur la portée de la Charte des droits fondamentaux de l'Union européenne. La portée limitée qui lui est reconnue par son article 51, paragraphe 1[70] a en effet donné naissance à une jurisprudence particulièrement pointilliste, marqué par nombre de non-dits et d'incohérences. A cela, rien de surprenant : comme le rappelle Dominique Ritleng, la délimitation du champ d'application de la Charte renvoie à l'épineuse *« question fédérale »*[71] de l **a répartition verticale des compétences et de la possible transformation de la Cour de justice en une nouvelle Cour européenne des droits de l'homm**e, et de la Charte en une *« Convention Européenne des Droits de l'Homme bis »*.[72] La problématique est d'autant plus épineuse qu'avant même l'entrée de la Charte, la jurisprudence de la Cour relative aux Principes Généraux du Droit de l'Union - que la Charte codifie pour partie - était elle-même largement fluctuante. Celle-ci oscillait en effet entre une conception restrictive de leur champ d'application impliquant que ceux-ci n'auraient vocation à s'appliquer que *« lorsqu'ils mettent en œuvre des réglementations communautaires »*[73] et une conception plus large, selon laquelle une réglementation nationale se trouve placée sous l'empire des droits fondamentaux *« dès lors [qu'elle]* ***entre dans le champ d'application*** *du droit communautaire »*[74].

34 Le retentissant arrêt *Akerberg et Fransson*[75] de 2013 avait semblé **trancher définitivement en faveur d'une conception large de ce champ d'application**, en énonçant que l'article 51, § 1 de la Charte implique qu'une mesure nationale constitue une *« mise en oeuvre »* du droit de l'Union, dès lors qu'elle se situe *« dans le cadre »* du droit de l'Union ou entre *« dans le champ d'application »* de ce droit ; ce qui implique non seulement que la charte lie les États membres agissant tels des agents de l'Union, mais également lorsque ceux-ci entendent déroger au droit de l'Union. Le caractère plastique et indéterminé de la notion

de *« champ d'application »* du droit de l'Union et la jurisprudence ultérieure démontre néanmoins que **la clarté de cette formulation était pour le moins obscure**

35 Ainsi, comme le rappelle le professeur Florence Benoit-Rohmer[76], le critère de *« mise en oeuvre »* du droit de l'Union utilisé par la Cour exige l'existence d'un *« lien entre une règle du droit interne et une disposition du droit de l'Union européenne ne doit pas être purement théorique »*. Plus précisément, la Cour a rappelé dans son arrêt *Siragusa* du 6 mars 2014[77] qu'une situation juridique doit à ce stade présenter *« un lien de rattachement d'un certain degré, dépassant le voisinage des matières visées ou les incidences indirectes de l'une des matières sur l'autre »*. Parmi les éléments à prendre en compte pour apprécier ce lien de rattachement – mentionnés par un arrêt *Ymeraga* du 8 mai 2013[78] – figure notamment le fait de savoir si la législation nationale a pour *« but de mettre en oeuvre une disposition du droit de l'Union »* et *« si celle-ci ne poursuit pas des objectifs autres que ceux couverts par le droit de l'Union, même si elle est susceptible d'affecter indirectement ce dernier »*. Contre toute attente, l'adoption en 2013 d'une formulation permettant un élargissement du champ d'application de la Charte **n'est pas exclusif d'une application restrictive de la Charte,** si bien qu'il apparaît bien difficile de cerner de manière satisfaisante les contours de sa portée.

36 L'arrêt *Willems* contribue à entretenir ce *hiatus*. Après avoir conclu à l'inapplicabilité du règlement et de la directive aux *« autre[s] utilisation ou conservation [des données des passeports] en application de la législation nationale »*, la Cour en vient logiquement à la conclusion qu'*« il n'y a pas lieu de vérifier si les conservations et les utilisations des données biométriques à des fins autres que celles visées à l'article 4, paragraphe 3, de ce règlement sont conformes auxdits articles de la Charte »*[79]. Pour en parvenir à cette conclusion et comme cela a été rappelé précédemment, la Cour s'est fondée sur le considérant 4 du règlement qui énonce que les données biométriques sont rassemblées et conservées dans le support de stockage des passeports et des documents de voyage en vue d'émettre ces documents *« sans préjudice de toute autre utilisation ou conservation de ces données en application de la législation nationale des États membres. »*[80] . Mais force est de constater que la Cour **ne mobilise cette portion du règlement que d'une manière pour le moins sélective**, puisque le même considérant énonce également que les données collectées restent soumises à *« toute disposition pertinente du droit de l'Union Européenne «* , de sorte qu'il apparaît peu douteux que le règlement ait bien entendu placer les *« autres utilisations »* des données des passeports sous l'empire de la directive 95/46/CE et que l'un des objectifs du texte est bien, également, de c**oncilier l'ensemble des usages des données biométriques avec l'objectif de garantie de la vie privée des citoyens européens**. Il n'aurait fallu ici qu'un simple effort de reformulation de la question posée pour que la Cour puisse conclure *a minima* qu'un Etat-membre est bien conduit à « mettre en œuvre » le droit de l'Union Européenne lorsqu'il réutilise les données collectées dans le cadre du règlement, puisqu'il contribuerait dans cette hypothèse à assurer **la mise en œuvre de l'objectif de sauvegarde des droits fondamentaux des citoyens européens contre l'usage abusif de leurs données personnelles.**

B – Données personnelles et « constitutionnalisation » de la Charte : Un sifflet de fin de partie ?

37 En définitive, la réponse timorée de la Cour à la question posée par la juridiction de renvoi frappe d'autant plus qu'elle tranche très nettement avec l'audace dont celle-ci

avait su faire preuve par le passé dans son interprétation des articles 7 et 8 de la Charte des droits fondamentaux de l'Union Européenne, invalidant dans un premier temps la directive 2006/24/CE sur la conservation des données à caractère personnel et condamnant ainsi la surveillance de masse[81], puis consacrant dans un second un « droit a l'oubli » numérique au profit des internautes[82]. Tant et si bien que certains auteurs avaient cru voir dans les arrêts les plus récents de la Cour une preuve de plus de la « constitutionnalisation »[83] de la protection des données personnelles à l' échelle de l'Union européenne. Il est vrai que l'épineuse question de la protection de la vie privée a l'ère numérique dans un contexte de surveillance de masse paraissait particulièrement a même de contribuer a la création du « patriotisme constitutionnel » que d'aucuns, y compris au sein de la Cour, appelaient de leurs vœux.

38 En effet, la révélation des programmes de surveillance des communications et les mobilisations de la société civile qu'ils ont suscité offraient en effet **l'occasion rêvée de mobiliser autour d'une supposée spécificité des valeurs européennes en la matière** en opposant au modèle nord-américain de protection des données personnelles une conception « humaniste » de la vie privée, que d'aucuns nomment désormais l' *« autodétermination informationnelle »*[84]. En somme, autant de « hard cases » en perspective pour les juridictions européennes. Ironie du sort, c'est **précisément a l'heure ou les programmes nord-américains de surveillance apparaissent partiellement remis en cause** par le congrès aux Etats-Unis[85] que la protection des données personnelles connaît un net reflux dans l'espace européen.

39 Loin de cet élan « patriotique », le jugement *Willems* semble au contraire, marquer le début d'un retrait de la Cour en ses quartiers s'agissant de la définition d'un socle « constitutionnel » de protection des données personnelles. En effet, en marquant son indifférence au sort des données collectées sur le fondement du règlement en raison de considérations (ou de prétextes ?) purement techniques relatives à l'absence de la démarche de la Cour tranche très nettement avec l'audace dont elle avait fait preuve dans l'arrêt *Digital Rights Ireland*[86]. Dans ce jugement « historique », la Cour avait, précisément, invalidé la directive 2006/24/CE parce que celle-ci n'allait pas assez loin **en ne mettant pas assez en œuvre les garanties adéquates susceptibles d'éviter un usage abusif des méta-données des internautes par les États membres.** Se prononçant sur la nécessité de l'ingérence dans le droit à la vie privée prévu par la directive, la Cour avait rappelé, en raisonnant par analogie avec la jurisprudence de la CEDH[87] que le droit de l'Union se doit de *« prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences«*[88] afin que les personnes dont les données ont été conservées *« disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »*, notamment lorsque les données à caractère personnel sont soumises à un traitement automatique car il existe, dans cette hypothèse, *« un risque important d'accès illicite à ces données »*[89].

40 En l'espèce, la Cour avait fait grief à l'article 4 de cette directive de ne pas disposer expressément que l'utilisation ultérieure des données en cause doive être *« strictement restreint à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci »*. En somme, la Cour avait, dans cet arrêt, **mené un raisonnement exactement inverse** à celui mené dans l'affaire *Willems* : elle n'avait pas tiré parti de l'absence de précision du droit de l'Union pour en conclure à l'inapplicabilité de la Charte. Bien au contraire, la directive avait été invalidée, parce qu'elle **n'encadrait**

pas de garanties suffisantes les usages que pouvaient faire les Etats-membres des données collectées. Comme l'avait souligné l'avocat général *Villalon*, la « précision de la loi » en matière de vie privée doit aller *« au-delà d'une exigence purement formelle pour appréhender le défaut de précision de la loi (« qualité de la loi ») [pour] l'exprimer dans les termes les plus simples possibles »*[90] . En clair, conformément à l'approche de la Cour européenne des droits de l'homme en la matière, l'imprécision d'une directive s'agissant de l'encadrement des usages ultérieurs des données collectées sur son fondement devrait, en principe, emporter invalidation de celle-ci, faute de satisfaire à l'exigence de précision mise en évidence par l'avocat général Villalon.

41 Certes, il paraissait bien difficile pour la Cour d'invalider le règlement de la même manière qu'elle avait invalidé la directive de 2006, puisque le précédent Schwartz avait précisément validé l'ensemble du règlement au regard des articles 7 et 8 de la Charte. Toutefois, l'arrêt Schwartz était largement réduit dans son champ d'application et la Cour aurait parfaitement pu, - comme elle l'a fait par le passé[91] - confronter un éventuel usages ultérieure de ces données à des fins autres que celles prévues par le règlement à la directive 95/46.CE lue *« à la lumière »* des articles 7 et 8 de la Charte. Et, dans ce cadre, celle-ci aurait parfaitement pu émettre une réserve quant à l'usage ultérieur des données en cause.

42 Mais si la jurisprudence de la Cour paraît en retrait, peut-être est-ce précisément parce qu'elle n'a jamais été d'une parfaite limpidité ? En effet, comme l'a remarqué Gloria Gonzalez-Fuster[92], la « saga » des arrêts de la Cour en matière de protection de la vie privée a certes affirmé les contours d'un véritable « droit à » la protection des données personnelles, **mais ces contours n'en restent pas moins incertains et fuyants**. Ainsi, si les juges du plateau de Kirchberg ont érigé le « droit à la protection des données personnelles » en droit autonome dans l'arrêt *Commission contre Bavarian Lager*[93], ceux-ci n'ont par la suite j**amais explicitement séparé le *« droit à la vie privée »* garantit par l'article 7 de la Charte, et le *« droit à la protection des données personnelles »*** garantit par l'article 8. Et, en analysant généralement les deux droits comme formant un droit plus général à la vie privée, la Cour a souvent été amenée soit à admettre plus largement des atteintes à la vie privée -ignorant très largement la portée de l''article 52§1 du TFUE[94]- , sans pour autant que les garanties issues de l'article 8 de la Charte ne soit explicitées de manière parfaitement claire. Or, cette imprécision de la jurisprudence de la CJUE en la matière présente le risque **d'affaiblir les protections instaurées dans le cadre de la jurisprudence européenne relative à la « vie privée »** au profit d'un « droit à la protection des données » personnelles dont les contours apparaissent largement indéfinissables. Les arrêts *Willems* et *Schwarz* sont à cet égard parfaitement limpides : citant abondamment la jurisprudence de la CEDH et en particulier son arrêt *Marper*, la Cour n'y applique pas pour autant les principes relatifs à la vie privée avec la même rigueur que son homologue strasbourgeoise. Curieuse conception du dialogue juridictionnel en matière de vie privée : **si la chèvre accepte d'être farcie de chou, c'est ainsi donc *« pour mieux se voir transformée en chou »***[95]**.**

*

* *

Conclusion : Vers une « Balkanisation » du droit à la protection des données personnelles dans l'ordre juridique de l'Union Européenne ?

43 Les considérations qui précèdent, qui n'ont ni la prétention d'être exhaustives, ni celle de fournir une clé de lecture unique des conséquences de l'arrêt Willems, témoignent de l'ampleur des problématiques ignorées par la Cour de Justice. A cet égard, l'arrêt rendu par la Cour laissera un sentiment de perplexité, et d'amertume.

44 Perplexité en premier lieu sur le plan de la protection des données de nature biométrique stricto-sensu, car le jugement de la CJUE semble faire fi des risques liés à l'explosion des usages des données biométriques. Or, ceux-ci apparaissent démultipliés par l'émergence de la « seconde génération » de technique biométriques – à savoir les techniques biométriques « soft »[96] qui utilisent des traits caractéristiques tels que le genre, le poids, la taille, l'âge - et ouvrent plus que jamais la voie à un profilage indistinct des individus sur le fondement de critères potentiellement discriminants. Les exemples de l'usage de ce type de techniques par des acteurs économiques démontrent d'ailleurs à quel point celles-ci peuvent générer des discriminations.[97] Ces risques accrus ont d'ailleurs conduit l'Assemblée parlementaire du Conseil de l'Europe à recommander aux Etats parties à la Convention 108 sur la protection des données personnelles de revoir leur législation en la matière[98] . Sur ce point, la démarche frileuse de la Cour apparaît largement contraire à l'objectif de dialogue entre les deux systèmes de protection des droits de l'homme.

45 Perplexité également, et plus généralement, sur le plan de la protection des droits fondamentaux dans le cadre de l'Union européenne. En effet, si tant d'auteurs avaient cru déceler dans les récents jugements de la Cour un démarche « constitutionnelle », c'est également que la création et la mise en œuvre juridictionnelle d'un catalogue de droits fondamentaux propres au droit de l'Union européenne pouvait apparaître sans aucun doute comme ayant plus d'impact que la simple référence aux traditions constitutionnelles des Etats membres et à la Convention européenne des droits de l'homme. Mais une telle *« constitutionnalisation »* des droits fondamentaux par le truchement d'un texte aussi *« puissant et ouvert à l'interprétation »* conduit également, comme l'ont rappelé de manière pertinente les professeurs Murphy et Anderson[99], à devoir placer une confiance énorme en la capacité de la Cour à assumer pleinement son rôle de gardien des droits fondamentaux dans l'ordre de l'Union Européenne. A cet égard, les incertitudes quant à la démarche de la Cour s'agissant de la définition du champ d'application de la Charte dont témoignent l'arrêt commenté porte en elle le germe le risque de *« balkanisation »* de la protection des droits de l'Homme dans l'espace européen que dénonçait un ancien membre la Cour[100]. Affirmant de manière très nette l'autonomie du droit de l'UE, pour *in fine* ne pas exercer pleinement son office, la Cour s'expose inévitablement et légitimement à la critique. Ne peut-on pas en effet considérer qu'une telle démarche pourrait, à terme, fragiliser l'ensemble du système européen de protection des droits de l'homme ?

46 Amertume enfin quand aux conséquences concrètes à moyen terme de la décision Willems, car la protection des citoyens européens contre la constitution de telles bases de données reposait sur un équilibre précaire désormais rompu. La rupture de cet équilibre apparaît d'autant plus dommageable qu'à l'heure où la « menace terroriste » et le « risque

migratoire » justifient des entorses croissantes aux libertés publiques, le risque d'une généralisation de la « biosurveillance » n'apparaît plus seulement hypothétique. Et, comme l'a démontré la retentissante affaire « Snowden », la déterritorialisation des contrôles des Etats sur les populations participe de la globalisation de la biométrie[101], si bien que s'esquissent sans cesse les contours d'une véritable biopolitique globalisée dans laquelle le réfugié et le national que tout semble opposer se voient confrontés à une problématique commune : celle de n'avoir « *nulle part où se cacher* »[102].

47 **CJUE, Quatrième chambre, 16 avril 2015, *W.P Willems c. Burgemeester Van Nuth*, aff. n ° C-446/12 à C-449/12**

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Règlement (CE) n° 2252/2004 du Conseil, du 13 décembre 2004, établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres (JO L 385, p. 1), tel que modifié par le règlement (CE) n° 444/2009 du Parlement européen et du Conseil, du 6 mai 2009.

2. "Le présent règlement s'applique aux passeports et aux documents de voyage délivrés par les États membres. Il ne s'applique pas aux cartes d'identité délivrées par les États membres à leurs ressortissants ou aux passeports et aux documents de voyage temporaires ayant une validité inférieure ou égale à douze mois "

3. Aux fins du présent règlement, les éléments biométriques des passeports et des documents de voyage ne sont utilisés que pour vérifier :a)l'authenticité du document ;b)l'identité du titulaire grâce à des éléments comparables directement disponibles lorsque la loi exige la production du passeport ou d'autres documents de voyage

4. CJUE, 4e Ch., 17 octobre 2013. Michael Schwarz contre Stadt Bochum, Aff. C-291/12. V. Le commentaire de EU Law radar sur l'arrêt. V. Également Evanthia Chatziliasi, et Athena Bourka. " Remarks and Considerations on the CJEU Decision on Biometric Passports.", in *Protecting the Genetic Self from Biometric Threats: Autonomy, Identity, and Genetic Privacy: Autonomy, Identity, and Genetic Privacy*, 2015, p. 223.

5. V.Katitza Rodriguez, « Highest Court in the European Union To Rule On Biometrics Privacy », Electronic Frontier Foundation, 15 octobre 2012.

6. Il s'agit du "droit d'être laissé seul/à l'écart" (right to be left alone), expression mentionnée pour la première fois par les juges Brandeis et Warren dans un article de 1890, duquel l'on fait dater formellement l'idée de « droit à la vie privée ». V. Neil M.

Richards, "The Puzzle of Brandeis, Privacy, and Speech", Vanderbilt Law Review, v.63, n.5, pp. 1295-1352.

7. V. G29, 20 juin 2007, Avis 4/2007 sur le concept de donnée à caractère personnel, WP 136

8. V. généralement, sur les risques suscités par ce type de techniques : Paul De Hert, Wim Schreurs et Evelien Brouwer. "„Machine–readable identity documents with biometric data in the EU–part IV “." *Keesing Journal of Documents & Identity,* 2007, n° 24.

9. *« Le recours à la biométrie dans les systèmes d'information n'est jamais anodin, surtout si le nombre d'individus concernés est très important. [E]n rendant possible la mesure des caractéristiques du corps humain par des machines et en permettant l'utilisation ultérieure de ces caractéristiques, la biométrie modifie définitivement la relation entre corps et identité. Même si les données biométriques ne sont pas accessibles à l'œil nu, des outils appropriés en permettent la lecture et l'utilisation, pour toujours et où que puisse se rendre la personne concernée. »* V. Contrôleur européen des données, Avis du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (JO C 181, p. 13)

10. V. G29, 4 octobre 2012, Avis 3/2005 sur l'application du règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, WP 112

11. V. par exemple, sur l'uage de la biométrie en lieu de travail : CNIL, Délibération n° 2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail

12. Cour.EDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04. V., sur cet arrêt : Sylvie Peyrou-Pistouley, « L'affaire *Marper c/ Royaume-Uni* : un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne », *RFDA* 2009, p. 94 ; Rocco Bellanova et Paul De Hert, « Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », *Cultures & Conflits* [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011,

13. *"Particulièrement préoccupant en l'occurrence est le risque de stigmatisation, qui découle du fait que les personnes dans la situation des requérants, qui n'ont été reconnus coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence, sont traitées de la même manière que des condamnés. Il convient de ne pas perdre de vue à cet égard que le droit de toute personne à être présumée innocente que garantit la Convention comporte une règle générale en vertu de laquelle on ne peut plus exprimer de soupçons sur l'innocence d'un accusé une fois que celui-ci a été acquitté"* V.Cour.EDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04, §122

14. JO C 98 du 23.4.2004, p. 39.

15. Résolution législative du Parlement européen sur la proposition, présentée par la Commission, de règlement du Conseil établissant des normes pour les dispositifs de sécurité et les éléments biométriques intégrés dansles passeports des citoyens de l'UE (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)),

16. Parlement Européen, Commission Libé, 25 octobre 2004, Biometrics at the Frontiers : Assessing the impact on Society,EC-DG JRC-IPTS

17. La question de la protection des données biométriques dans les Etats-members de l'Union dépasse largement les frontières de cette étude et ne sera donc pas abordée. Néanmoins, les études menées sur la question démontrent de très importantes divergences d'approche, de sorte que le jugement Willems conduit à accroître l'inégalité des justiciables Européens en la matière.

V. Conseil de l'Europe. « Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data »*Strasbourg,* Février 2005; « Biometric identification and Privacy », Comparative research prepared by Oxford Pro Bono Publico for the Centre for Law and Policy Research, India, février 2013.

18. Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres [Voir acte(s) modificatif(s)].

19. CJUE, 4e Ch., 17 octobre 2013, Michael Schwarz contre Stadt Bochum, aff.C.291/12, V;Evanthia Chatziliasi, Athena Bourka, « Remarks and Considerations on the CJEU Decision on Biometric Passports » in Christina Akrivopoulou (dir.), Protecting the Genetic Self from Biometric Threats, p. 223

20. CJUE, 3e Ch., 24 novembre 2011, ASNEF et FECEMD, Aff. C-468/10 et C-469/10, § 38 et 40. V. Fabienne Fauff-Gazin, Directive "protection des données", Europe n° 1, p. 14-15 ; Anne Debet, Précisions européennes sur les fondements légitimes des traitements de données personnelles, Commerce Communications Electroniques, p. 32-34.

21. CJUE, Gr. Ch, 9 novembre 2010, Volker und Markus Schecke et Eifert, Aff. C-93-09. V. Stefan Huber et Hans Kristoferitsch, « Transparency : Let There Be Light ? Comments on the Judgment of the European Court of Justice, Joined Cases C-92/09 and C-93/09 », *European Food and Feed Law Review : Ep.FFL*, 2011, vol. 6, no 4, p. 687 ; Isabelle Andoulsi, « L'arrêt de la cour du 9 novembre 2010 dans les affaires jointes Volker und Markus Schecke GBR et Hartmut Eifert contre Land d'Hessen (C-92/09 et C-93/09) : une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles ? « , Cahiers de droit Européen - n° 2, p. 471-522 ; Elise Degrave, « Arrêt Volker und Markus Schecke et Eifert : le droit fondamental à la protection des données à caractère personnel et la transparence administrative « , Journal de droit européen n° 78, pp. 97-99

22. Cour.EDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04, §68

23. CJUE, Gr. Ch, 9 novembre 2010, Volker und Markus Schecke et Eifert, Aff. C-93-09, §52

24. Le raisonnement de la Cour sur ce point apparaît en effet tautologique et peu convaincant, considérant l'ingérence comme " prévue par la loi" au motif qu'elle a été encadrée par le règlement, sans examiner si les garanties offertes par le règlement peuvent ou non être considérées comme suffisantes. V. CJUE, 4e Ch., 17 octobre 2013, Michael Schwarz contre Stadt Bochum, aff.C.291/12, Point 35 : *"En l'occurrence, il est constant, premièrement, que la limitation qui résulte du prélèvement et de la conservation d'empreintes digitales dans le cadre de la délivrance de passeports doit être considérée comme étant prévue par la loi, au sens de l'article 52, paragraphe 1, de la Charte, dès lors que l'article 1er, paragraphe 2, du règlement no 2252/2004 prévoit ces opérations"*

25. CJUE, 4e Ch., 17 octobre 2013, Michael Schwarz contre Stadt Bochum, aff.C.291/12

26. La Cour avait surtout constaté, sur ce point, que les requérants n'avaient pas présenté de technique alternative moins intrusive et présentant un degré de fiabilité équivalent. CJUE, 4e Ch., 17 octobre 2013, Michael Schwarz contre Stadt Bochum, aff.C.291/12, § 51 : *« D'autre part, il y a lieu de relever que la seule réelle alternative au prélèvement des empreintes digitales évoquée au cours de la procédure devant la Cour consiste dans la saisie d'une image de l'iris de l'œil. Or, rien dans le dossier soumis à la Cour n'indique que ce dernier procédé soit moins attentatoire aux droits reconnus par les articles 7 et 8 de la Charte que le prélèvement des empreintes digitales. «*

27. Cour.EDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04, §103

28. CJUE, 4e Ch., 17 octobre 2013, Michael Schwarz contre Stadt Bochum, aff.C.291/12, § 61 et 62

29. Conclusions de l'avocat général Paolo Mengozzi présentées le 13 juin 2013, Michael Schwarz contre Stadt Bochum, Affaire C-291/12, § 56

30. Idem, §58 : *« Alors, oui, l'identification par la comparaison des empreintes digitales est une technique qui connaît des limites et, non, il ne m'est pas possible de dire que le règlement no 2252/2004 tel que modifié a mis en place un régime permettant d'exclure, de manière absolue, tout risque, y compris en termes d'utilisation frauduleuse et de contrefaçon. Cela étant, [...] le législateur a pris toutes les mesures nécessaires afin de garantir, dans toute la mesure du possible, le traitement loyal et licite des données personnelles requises pour la délivrance d'un passeport. »*

31. Idem, § 55 *« Quant aux États tiers, je ne partage pas l'avis du requérant selon lequel l'article 1er, paragraphe 2, du règlement no 2252/2004 tel que modifié serait la cause de l'exposition des citoyens de l'Union au risque d'abus encouru dans ces États. Il suffit, à cet égard, de constater que l'Union n'a pas d'influence sur la détermination des formalités à accomplir par ses citoyens pour l'entrée sur le territoire des États tiers «*

32. Idem, §55

33. CJUE, Quatrième chambre, 16 avril 2015, W.P Willems c. Burgemeester Van Nuth, aff. n ° C-446/12 à C-449/12, §47

34. Idem, §48

35. V .Steve Peers, « Biometric data and data protection law: the CJEU loses the plot », EU Law analysis, 17 avril 2015. V. également: Eduardo Gil-Pedro, « Joined Cases C-446/12 – 449/12 Willems: The CJEU washes its hands of Member States' fingerprint retention », EU Law Blog, 29 avril 2015.

36. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

37. Article 6 : 1. Les États membres prévoient que les données à caractère personnel doivent être : [...]b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées [...] «

38. CJUE, Quatrième chambre, 16 avril 2015, W.P Willems c. Burgemeester Van Nuth, aff. n ° C-446/12 à C-449/12, §1

39. CJUE, 29 janvier 2008, Promusicae, Aff. C-275/06, Rec. p. I-271. V.Olivier de Schutter, " Les droits fondamentaux dans l'Union européenne ## (1 er février 2008-1 er février 2009) ", Journal de droit européen, n° 158, p. 115-121.

40. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur

41. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

42. CJUE, 4e Ch., 17 octobre 2013, Michael Schwarz contre Stadt Bochum, aff.C.291/12, §29

43. "L'exigence de prévisibilité a trouvé une expression particulière dans le droit de la protection des données qui impose que tout traitement de données soit lié à des fins déterminées, comme

l'exige expressément l'article 8, paragraphe 2, de la charte ". V. Conlusions de l'avocat général Mme Juliane Kokott, 18 juillet 2007, Promusicae contre contre Telefónica de España SAU, Affaire C-275/06, §53

44. Conclusions de l'avocat général M. Niilo Jääskinen, 17 novembre 2011, Bonnier Audio AB contre Perfect Communication Sweden AB (« ePhone »), Affaire C-461/10, §51

45. G29, 2 avril 2013, Opinion 03/2013 on purpose limitation, WP 203.

46. Idem, p. 23

47. Idem, p. 24

48. Idem, p. 26

49. Et ce d'autant plus que les requérants eux-même pointaient du doigt les risques de sécurité liés à la création d'une base de données de police centralisé aux Pays-Bas.

50. Cour EDH, 28 mars 1987, Leander c. Suède, § 48, série A no 116

51. Cour EDH, Gr. Ch., Amann c. Suisse, Req. n° 27798/95, § 69, CEDH 2000-II

52. Cour EDH,4e Sect., 28 janvier 2003, Peck c. Royaume-Uni , Req. No 44647/98, § 59

53. Cour EDH, 3e Sect.,25 septembre 2001, P.G et J.H c. Royaume-Uni, Req. no 44787/98, §§ 59-60, CEDH 2001-IX

54. Cour.EDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04, §89

55. Idem.

56. V. également, sur ce point : Cour EDH, 24 avril 1990, Kruslin c. France, §§ 33 et 35, série A no 176-A, Cour EDH, 4 mai 2000, Rotaru contre Roumanie, §§ 57-59, Cour EDH, 28 juin 2007, Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie, Req. no 62540/00, §§ 75-77, Cour EDH, 1er juillet 2008, Liberty et autres c. Royaume-Uni, no 58243/00, §§ 62-63.

57. V. sur ce point, la Recommandation no R (92) 1 du Comité des Ministres du Conseil de l'Europe sur l'utilisation des analyses de l'ADN dans le cadre du système de justice pénale

58. V., pour une tentative de séparer conceptuellement les deux droits : Paul De Hert ,Serge Gutwirth, "Data protection in the case law of Strasbourg and Luxemburg : Constitutionalisation in action", In *Reinventing data protection ?*. Springer Netherlands, 2009. p. 3-44.

59. V. sur ce point: Tomas Gomez-Arostegui, « Defining private life under the European convention on human rights by referring to reasonable expectations », *California Western International Law Journal*, 2005, vol. 35, no 2.

60. V. Peter Winn, Katz and the Origins of the Reasonable Expectation of Privacy Test. *McGeorge L. Rev.*, 2009, vol. 40, p. 1.;, Haley Plourde-Cole," Back to Katz: Reasonable Expectation of Privacy in the Facebook Age", *Fordham Urban Law Journal*, 2010, vol. 38.

61. Cour EDH, 25 juin 1997, Halford c. Royaume-Uni, Req. no 20605/92

62. Cour EDH, 4e Sect., 3 avril 2007, Copland c. Royaume-Uni, Req. no 62617/00

63. Cour EDH, 4e Sect., 28 janvier 2001, Peck c. Royaume-Uni, Req. no 44647/98 §62

64. V. Conlusions de l'avocat général Mme Juliane Kokott, 18 juillet 2007, Promusicae contre contre Telefónica de España SAU, Affaire C-275/06, §53

65. Cour EDH, 14 mars 2002, Gaweda c. Pologne, Req. n° 26229/95

66. V. Peter Omtizgt, « Les opérations massives de surveillance en Europe », Conseil de l'Europe, CDCJ(2014), AS/Jur(2015)01, Strasbourg, janvier 2015 ; « La protection des donneurs d'alerte », Conseil de l'Europe, CDCJ(2014), AS/Jur (2015) 06.

67. Cour EDH, 26 avril 1985, Malone c. Royaume-Uni, Requête no 8691/79

68. V.Jillyanne Redpath, « Biometrics and international migration », in*ANNALI-ISTITUTO SUPERIORE DI SANITA*, 2007, vol. 43, no 1, p. 27.

69. V. Simon McGarr, Do Facebook and the USA violate EU data protection law? The CJEU hearing in Schrems, EU Law Analysis, 29 mars 2015

70. *"2. La présente Charte n'étend pas le champ d'application du droit de l'Union au-delà des compétences de l'Union, ni ne crée aucune compétence ni aucune tâche nouvelles pour l'Union et ne modifie pas les compétences et tâches définies dans les traités.* "V. également Les explications du praesidium relatives à la charte (2007/C 303/02)

71. Dominique Ritleng, « De l'articulation des systèmes de protection des droits fondamentaux dans l'Union », *RTD eur*. 2013. 267

72. Idem

73. CJCE, 13 juillet 1989, Hubert Wachauf c. Bundesamt für Ernährung und Forstwirtschaft , aff. 5/88, Rec. p. 2609, point 19

74. CJCE, 18 juin 1991, Elliniki Radiophonia Tiléorassi AE (ERT), aff. C-260/89, Rec. p. I-2925, point 42

75. CJUE, Gr. Ch, 7 mai 2013, Akerberg et Fransson, aff. C-617/10 Sébastien Platon, « La Charte des droits fondamentaux et la « mise en œuvre » nationale du droit de l'Union : précisions de la Cour de justice sur le champ d'application de la Charte »RDLF 2013, chron. N° 11 ; Laure Clément-Wilz, Francesco Martucci et Coralie Mayeur-Carpentier, « Chronique de droit administratif et droit de l'Union européenne », *RFDA* 2014, p. 985 ; Emmanuelle Broussy, Hervé Cassagnabère et Christian Gänser « Chronique de jurisprudence de la CJUE » *AJDA* 2015, p. 1093 :

76. V. Florence Benoit-Rohmer, « Champ d'application de la Charte (article 51 de la Charte), *RTD eur*. 2015, p. 161 ;

77. CJUE, 10e Ch, 6 mars 2014, Cruciano Sirgusa, aff. C-206/13

78. CJUE, 8 mai 2013, Ymeraga ,aff. C -87/12, § 41)

79. CJUE, 4e Ch., 17 octobre 2013, Michael Schwarz contre Stadt Bochum, aff.C.291/12, §47

80. Idem, §48

81. CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12. V. Florence Benoit-Rohmer, « Protection des données personnelles ; Note sous Cour de justice de l'Union européenne, grande Chambre, 8 avril 2015, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres et Kärnter Landesregierung Seitlinger et autres, affaires jointes numéros C-293/12 et C-594/12 », *RTDE* 2015, p. 168 Denys Simon, « La révolution numérique du juge de l'Union : les premiers pas de la cybercitoyenneté », *Europe* n° 7, p. 4 ; Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », in *Revue des droits de l'homme*, 14 mai 2014

82. CJUE, Grande Chambre, 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, Aff. C-131/12 – Communiqué de presse et ADL du 16 juin 2014

83. V. Steve Peers, Data retention: a landmark court of justice's ruling (4). Will this saga continue and how? », European Law Blog, 8 avril 2014.

84. La notion d' « *autodétermination informationnelle* », s'oppose à une conception patrimoniale des données personnelles et inscrit la protection de l'autonomie individuelle dans une approche par les droits de l'homme. Chaque sujet de droit aurait désormais un droit à « *la maîtrise de la circulation « légitime » de son image informationnelle.* ».

V.Antoinette Rouvroy, *« Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? », in Stéphanie Lacour (dir.), La sécurité de l'individu numérisé. Réflexions prospectives et internationales, Paris, L'Harmattan, 2009, p. 2.*

85. Le Freedom Act adopté le 22 juin 2015 met en effet formellement fin aux programmes dénoncés par Edward Snownde

86. CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12

87. Cour EDH, 4 mai 2000, Rotaru contre Roumanie, §§ 57-59, Cour EDH, 28 juin 2007, Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie, Req. no 62540/00 , §§ 75-77, Cour EDH, 1er juillet 2008, Liberty et autres c. Royaume-Uni, no 58243/00, §§ 62-6

88. CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12, §54

89. Idem.

90. Conclusions de l'avocat général Villalon sur l'affaire Digital Rights Ireland, présentées le 12 décembre 2013 , Affaire C-293/12

91. Celle-ci avait dégagé un « droit à l'oubli » au profit des internautes en raisonnant de cette manière dans l'arrêt Google Spain. V.CJUE, Grande Chambre, 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, Aff. C-131/12 – Communiqué de presse et ADL du 16 juin 2014

92. Gloria Gonzàlez Fuster, « Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection »,Birkbeck Law Review Volume 2(2), p. 263.

93. CJUE, Gr. Ch, 29 juin 2010, Commission c. Bavarian Lager, Aff. C-28/08

94. *1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.*

95. V. Véronique Champeil-Desplats, « Les droits fondamentaux et l'identité des ordres juridiques : l'approche publiciste », in *Edouard Dubout, Sébastien Touzé, « Les droits fondamentaux : Charnières entre ordres et systèmesjuridiques », Paris, Pedone,* 2010, p. 156

96. Marx G.T., « Soft Surveillance. The Growth of Mandatory Volunteerism in Collecting Personal Infomation - "Hey Buddy Can You Spare a DNA?" », in Monahan T. (ed.), *Surveillance and Security. Technological Politics and Power in Everyday Life*, New York/London, Routledge, 2006, pp. 37-56.

97. V. Comité des Ministres du Conseil de l'Europe, 18 septembre 2002, Recommandation n° R (2002) 9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance.

98. V.Assemblée parlementaire du Conseil de l'Europe, Résolution 1797 (2011) sur la nécessité de mener une *réflexion mondiale* sur les implications de la biométrie pour les droits de l'homme, Strasbourg, 11 mars 2011.

99. David Anderson et Cian Murphy, »The Charter of Fundamental Rights: History and Prospects in Post-Lisbon Europe » 2011.

100. Obituary: Lord MacKenzie-Stuart', The Guardian,25 Mai 2000. Cité dans: Christopher Vajda, « The Application of the EU Charter of Fundamental Rights: Neither Reckless nor Timid? », 18 novembre 2014, Edinburgh School of Law Research Paper No. 2014/47.

101. Philippe Bonditti, « Biométrie et maîtrise des flux : vers une « géo-technopolis du vivant-en-mobilité » ? », *Cultures & Conflits* [En ligne], 58 | été 2005, mis en ligne le 10 octobre 2005, consulté le 12 juin 2015. : Ayse Ceyhan, « Enjeux d'identification et de surveillance à l'heure de la biométrie », *Cultures & Conflits* [En ligne], 64 | hiver 2006, mis en ligne le 02 avril 2007.

102. V. Glenn Greenwald, "Nulle part où se cacher", JC Lattès, Paris, mai 2014.

RÉSUMÉS

Le 16 avril 2015, la Cour de Justice de l'Union Européenne a refusé de garantir que les empreintes digitales rassemblées sur le fondement du règlement n° 2252/2004 (relatif aux passeports biométriques) de l'Union Européenne ne seront pas utilisées à des fins autres que la délivrance du passeport ou autre document de voyage biométrique. Surtout, et par un raisonnement pour le moins spécieux, la Cour ne place les données biométriques en cause ni sous l'empire de la Charte des droits fondamentaux de l'Union Européenne, ni sous celui de la directive 1995/46/CE protégeant les données personnelles. Ainsi, par une lecture restrictive de son précédent arrêt Schwartz de 2013, la Cour se lave les mains du destin des empreintes digitales collectées sur le fondement du droit dérivé de l'Union Européenne. Ce faisant, elle vide tragiquement la portée du droit à la protection des données personnelles dans un domaine où celui-ci est vital. Et, au-delà, la vision restrictive de la portée de la Charte des droits fondamentaux que mettent en œuvre les juges dans l'arrêt commenté suscite nombre d'incertitudes quant à la portée et à l'effet de la Charte des droits fondamentaux de l'Union Européenne, et notamment de ses articles garantissant le droit à la vie privée et le droit à la protection des données personnelles. Au risque d'affaiblir la force de ladite protection et d'ouvrir la voie à une « balkanisation » du régime européen de protection de la vie privée dans l'Union Européenne. Toutes proportions gardées, le présent jugement semble bien marquer le « glas » de la démarche constructive des juges de Luxembourg en matière de protection des données personnelles.

AUTEUR

JEAN-PHILIPPE FOEGLE

Doctorant en droit public (CREDOF - Université Paris Ouest Nanterre) et allocataire doctoral (Conseil régional d'Ile de France)